DIGITALEUROPE

Implementering af EU's direktiv om net- og informationssikkerhed (NIS)

Bruxelles, 5 Juli 2016

RESUMÉ

EU-Rådet har den 21. april 2016 offentliggjort den endelige version af direktivet om net- og informationssikkerhed (NIS). Selvom direktivet stadig skal godkendes formelt af Europa-Parlamentet til sommer, er de tre EU-institutioner nået til enighed om teksten, som ikke forventes at blive ændret yderligere. Medlemsstaterne er forpligtet til at gennemføre direktivet i deres nationale ret senest 21 måneder efter dets vedtagelse. Som en hjælp til denne proces indeholder vedlagte bilag en vejledning i bedste praksis for, hvordan de aspekter, der er relevante for teknologiindustrien, kan gennemføres, og hvordan der bedst tages højde for forfatternes hensigter.

EU's NIS-direktiv er den første paneuropæiske lovgivning om cybersikkerhed. Den sigter på at styrke de nationale cybermyndigheder og øge koordinationen imellem dem, og den indfører sikkerhedskrav til de vigtigste industrisektorer på området.

De nationale implementeringerbør ikke tabe direktivets to hovedformål af syne: (1) at sikre landets kritiske infrastrukturer et højt cybersikkerhedsniveau; (2) at etablere en effektiv samarbejdsmekanisme mellem EU-medlemsstaterne i dette øjemed. Ressourcerne skal først og fremmest bruges på at nå disse to vigtige mål.

For teknologiindustrien er bestemmelserne vedrørende de såkaldte udbydere af digitale tjenester (UDT'er) af særlig interesse. Direktivet angiver klart, at der er fundamentale forskelle på operatører af væsentlige tjenester (OVT'er) og UDT'er. Sidstnævnte betragtes således ikke som sådan som kritisk infrastruktur. Som det afspejles i lovgivningen ville en hændelse, der rammer disse digitale tjenester, udgøre en væsentligt lavere risiko for et lands økonomiske og offentlige sikkerhed. Det er vigtigt at opretholde denne forskel for at sikre en effektiv udnyttelse af de knappe ressourcer, som de myndigheder, der skal overvåge og håndhæve reglerne, råder over.

Vi anbefaler derfor, at der tages nøje højde for det tilsigtede omfang af de nævnte tjenester, og vi appellerer til de politiske beslutningstager om ikke at gøre andre sektorer end de, der identificeres som UDT'er eller OVT'er, til genstand for sikkerhedskrav i den nationale lovgivning.

Med hensyn til jurisdiktion skal UDT'er kunne regne med den lov, der gælder i det land, hvor de har deres hovedforretningssted, selv i sager der involverer kompetente myndigheder i mere end et land. Med hensyn til tilsyn bør de kompetente myndigheder anvende en ex post-tilgang i stedet for at pålægge en generel forpligtelse til at overvåge UDT'erne. De skal endvidere fokusere på resultaterne og opretholde forskellen mellem OVT'er og UDT'er ved ikke at pålægge sidstnævnte krav, som ikke indgår i direktivet, såsom auditering eller bindende instruktioner.

UDT'ernes sikkerhedsforanstaltninger skal være forskellige fra OVT'ernes, eftersom direktivet angiver, at UDT'erne udgør en væsentligt lavere sikkerhedsrisiko. Beslutningstagerne bør realisere målet om harmonisering for disse tjenester, anerkende eksisterende internationale industristandarder, undgå at påbyde teknologier, og overholde UDT'ernes ret i henhold til direktivet til at definere hvilke sikkerhedsforanstaltninger, der er mest

DIGITALEUROPE
Rue de la Science, 14 - 1040 Bruxelles [Belgien]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Medlem af Kommissionens åbenhedsregister: 64270747023-20

hensigtsmæssige for deres systemer. Hændelsesunderretning skal også være så harmoniseret som muligt på europæisk niveau. Den skal fokusere på hændelser, der påvirker tjenestens kontinuitet, tillade en fleksibel tidsplan for underretningen og skabe et tillidsmiljø, som indbyder til at dele information, uden at den underrettende part udsættes for øget risiko.

De foranstaltninger, der pålægges OVT'erne, vil også påvirke andre industrier, eftersom sikkerhedsforanstaltningerne og kravene om hændelsesunderretning vil blive udbredt gennem indgåelse af kontrakter med underleverandører. Dette gælder særligt for cloud-tjenester. Som følge heraf kan UDT'er indirekte blive underlagt deres kunders nationale love, og vi har derfor en stærk interesse i, at der gælder internationalt anerkendte sikkerhedsforanstaltninger for disse tjenester. Vi foreslår også koordination og synergi i så stort et omfang som muligt mellem kravene om underretning for både OVT'er og UDT'er, eftersom sidstnævnte sandsynligvis kan blive genstand for dobbelt underretning.

Direktivet har ambition om at nå et højt fælles sikkerhedsniveau for net- og informationssystemer med henblik på at forbedre det indre markeds funktion. For at nå dette høje mål skal **de nationale implementeringer fokusere på en risikobaseret, harmoniseret og international tilgang**. De skal give den private sektor tilstrækkelig fleksibilitet til at tilpasse sig til det hurtigt skiftende truselsbillede, tillade cybermyndighederne at fokusere deres begrænsede ressourcer på de vigtigste udfordringer, og huske på, at løsningen til et grænseoverskridendet problem nødvendigvis må være global. Vi håber, denne vejledning vil være et nyttigt værktøj i dette øjemed, og vi besvarer meget gerne alle yderligere spørgsmål.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Bruxelles [Belgien]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Medlem af Kommissionens åbenhedsregister: 64270747023-20

Bilag: Vejledning i bedste praksis for gennemførelse af NIS-direktivet

1. Udbydere af digitale tjenester

a) Anvendelsesområde

- I direktivet fastsættes det, at onlinemarkedspladser, onlinesøgemaskiner og cloud computing-tjenester skal betragtes som udbydere af digitale tjenester (UDT'er) og dermed være omfattet af direktivet. Selvom dette er et minimumsharmoniseringsdirektiv (Artikel 2), er det vigtigt at opretholde en ensartethed i hele EU, og medlemsstaterne bør ikke gøre andre sektorer end de, der er identificeret som UDT'er eller operatører af væsentlige tjenester (OVT'er), som defineret i artikel 3, til genstand for sikkerhedskrav i den nationale lovgivning.

- I direktivet anføres det udtrykkeligt, at hardwarefabrikanter og softwareudviklere ikke er OVT'er eller UDT'er og således ikke skal være underlagt de nationale love, der gennemfører direktivet (Betragtning 50).

- I direktivet udelukkes onlinetjenester, der fungerer som mellemled for tredjepartstjenester, hvor aftalen om salg eller tjenester i sidste ende indgås (fx sammenligningswebsteder), udtrykkeligt fra omfanget af onlinemarkedspladser (Betragtning15).

- Søgefunktioner, der er begrænset til indholdet af et bestemt websted, skal ikke betragtes som onlinesøgemaskiner, uanset om de anvender en ekstern udbyder (Betragtning 16).

- Definitionen af cloud computing-tjenester ifølge direktivet afhænger af, at IT-ressourcer deles af flere brugere (artikel 4(19) og Betragtning 17). I det omfang private clouds (i modsætning til offentlige clouds) er tilegnet en enkelt organisation, skal de ikke være omfattet.

- I direktivet understreges det, at der er grundlæggende forskelle på OVT'er og UDT'er, hvorfor UDT'er er underlagt andre regler (Betragtning 57). En sådan forskelsbehandling skal opretholdes ved gennemførelse af direktivet.

b) Jurisdiktion og tilsyn

- Jurisdiktionen for UDT'er bør kun tildeles til én medlemsstat, hvor operatøren har sit hovedforretningssted i EU, hvilket i princippet svarer til det sted, hvor operatøren har sit hovedkontor i EU (Artikel 18.1 og Betragtning 64). Vi mener, at UDT'erne selv skal kunne bestemme dette, og at denne beslutning kun skal kunne revideres, hvis de kompetente myndigheder bestrider den i forbindelse med ex post-tilsynsaktiviteter.

- Når UDT'er har net- og informationssystemer i andre lande end der, hvor deres hovedforretningssted er beliggende, forudses det i artikel 17.3, at de kompetente myndigheder samarbejder. Fra UDT'ernes synspunkt er det imidlertid vigtigt, at den gældende lov forbliver loven i deres hovedforretningssteds land, og at de forbliver alene ansvarlige over for den jurisdiktions kompetente myndighed, som de har kontakt med.

- I direktivet understreges det, at UDT'erne er underlagt et reaktivt ex post-tilsyn, og de kompetente myndigheder har således ingen generel forpligtelse til at føre tilsyn med UDT'erne. De bør kun skride til handling, når de har modtaget dokumentation. (Artikel 17.1 og Betragtning 60). Disse bestemmelser skal overholdes ved gennemførelse af direktivet.

- I modsætning til OVT'er kan myndighederne, for hvad angår UDT'er, kun rekvirere information og kræve, at UDT'erne afhjælper eventuelle mangler. I direktivet gøres det klart, at myndighederne ikke har nogen auditeringsbemyndigelse, og at de ikke kan udstede bindende instruktioner. Disse bestemmelser skal også overholdes på nationalt plan.

c) Yderligere krav

- Kravene til UDT'erne mht. sikkerhed og underretning er underlagt maksimal harmonisering (Artikel 16.10). Denne artikel skal også anses at gælde for de produkter, tjenester og løsninger, der udgør deres net- og informationssystemer. Yderligere bestemmelser, såsom om produkttestning, burde således ikke være nødvendige, og såfremt produkterne og tjenesterne anvendes i denne sammenhæng.

d) Sikkerhedsforanstaltninger og standarder

- Sikkerhedsforanstaltningerne for UDT'er skal være mere moderate end for OVT'er. UDT'er skal have frihed til at definere, hvordan de varetager sikkerheden, og hvordan de ønsker at sikre beskyttelsen af deres net- og informationssystemer svarende til de risici, de udsættes for (Betragtning 49).

- Sikkerhedsforanstaltningerne skal være procesorienterede og have fokus på risikostyring. De må ikke kræve, at informations- og kommunikationsteknologiprodukter (IKT-produkter) designes, udvikles eller fremstilles på en bestemt måde (Betragtning 51).

- I direktivet fremhæves det, at medlemsstaterne ikke må pålægge UDT'erne yderligere sikkerhedskrav (Artikel 16.10).

- Ikke desto mindre forventer vi retningslinjer fra en lang række aktører. Medlemsstaterne skal sørge for, at de foranstaltninger, der opridses i direktivet, vedtages (Artikel 16.1). De kan tilskynde til brugen af standarder til at gennemføre dem (Artikel 19.1) og drøfte standarderne med de europæiske standardiseringsorganisationer i samarbejdsgruppen (Artikel 11.3(h)). ENISA vil rådgive om egnede standarder (Artikel 19.2), og Europa-Kommissionen har ansvaret for at vedtage gennemførelsesretsakter om sikkerhedsforanstaltningerne (Artikel 16.8).

- I betragtning af komplikationsniveauet og fordelene ved harmonisering anbefaler vi, at den nationale proces i det væsentlige retter sig efter gennemførelsesretsakterne for at opnå enighed om de passende foranstaltninger, som i alle tilfælde skal være afgjort senest et år efter direktivets vedtagelse. Gennemførelsesretsakterne selv må ikke begrænse UDT'ernes mulighed for at definere de sikkerhedsforanstaltninger, der er bedst egnede for deres systemer.

- Artiklen om standardisering giver mulighed for at henvise til europæiske eller internationalt anerkendte standarder (Artikel 19.1). I betragtning af modenheden af de internationale standarder, der findes på

dette område, anbefaler vi, når egnede standarder findes, at en certificering i henhold til en af disse (såsom ISO 27001) er tilstrækkelig til at overholde kravene.

- Standardcertificering skal under alle omstændigheder være valgfri, ikke obligatorisk. I artikel 19 understreges det, at der kun kan "tilskyndes" til at benytte standarder, og at dette skal ske "uden at de påtvinger eller forskelsbehandler til fordel for anvendelse af en bestemt type teknologi".

e) Underretning om sikkerhedshændelser

- Som for sikkerhedsforanstaltningerne spiller en lang række parter en rolle i udformningen af hændelsesunderretningen ifølge NIS-direktivet. Medlemsstaterne skal sørge for, at UDT'erne underretter om de sikkerhedshændelser, der har betydelige konsekvenser for leveringen af den tjeneste (inden for direktivets anvendelsesområde), som de yder (Artikel 16.3). Samarbejdsgruppen har ansvaret for at drøfte metoderne for underretning (Artikel 11.3(m)), og Kommissionen har ansvaret for at vedtage gennemførelsesretsakterne (Artikel 16.8 og 9).

- Igen er det vores anbefaling, at de nationale gennemførelser retter sig efter processen i gennemførelsesretsakterne, hvoriblandt gennemførelsesretsakten om tærskler for underretning skal være vedtaget senest et år efter direktivets færdiggørelse.

- Hvad angår hvilke typer af hændelser, der skal underrettes om, pålægges UDT'erne at underrette om "enhver hændelse, der har betydelige konsekvenser for leveringen af [deres] tjeneste" (Artikel 16.3). Som for gennemførelsen af de tilsvarende bestemmelser for teleoperatører i Artikel 13a i rammedirektivet mener vi, dette skal fortolkes som en fokus på **kontinuiteten (eller tilgængeligheden)** af de leverede tjenester. Med andre ord skal afbrydelser indberettes, når de når en bestemt tærskel (som skal fastsættes i gennemførelsesretsakterne), snarere end enhver anden type sikkerhedshændelse. Dette har fordelen af at fokusere på de hændelser, som har størst sandsynlighed for at få konsekvenser for økonomien eller samfundet, samtidig med at overlappet med kravene om underretning om brud på persondatasikkerheden i henhold til den generelle forordning om databeskyttelse reduceres mest muligt.

- Desuden foreskriver underretningsforpligtelsen for operatører af væsentlige tjenester, at disse operatører skal underrette om "hændelser, som har betydelige konsekvenser for kontinuiteten af de væsentlige tjenester, de leverer", hvilket igen klart fokuserer på kontinuiteten (eller tilgængeligheden) af tjenesten. Medlovgiverne er enige om, at UDT'ernes forpligtelser skal være mere moderate end OVT'ernes (se Betragtning 49). UDT'ernes pligt til hændelsesunderretning i henhold til NIS må således ikke være mere omfattende end OVT'ernes, faktisk bør den være mere begrænset, hvad tærsklerne angår. Dette fremhæver igen, at UDT'ernes hændelsesunderretning skal være begrænset til hændelser, der når en vis tærskel, og som **påvirker kontinuiteten/tilgængeligheden af tjenesten,** og ikke hændelser vedrørende integriteten eller fortroligheden af data, som i vid udstrækning allerede er dækket af tilsvarende underretningskrav i henhold til den generelle forordning om databeskyttelse og eIDAS-forordningen.

- Med hensyn til tidsplanen for underretningen sætter vi pris på den fleksibilitet, der er antydet i udtrykket "hurtigst muligt" (Artikel 16.3). Gennemførelsen bør ikke indebære strengere tidsfrister, idet hændelsernes kompleksitet kan variere betydeligt. Ensartede underretningstider ville føre til unøjagtig underretning, når omfanget af de berørte systemer indledningsvis ikke er klart, og de ville have

konsekvenser for hændelsesresponsfagfolkenes evne til at prioritere responsen på hændelsen i forhold til at underrette om den.

- Som drøftet kan sikkerhedshændelser, der skal indberettes i henhold til direktivet, også skulle indberettes i henhold til databeskyttelsesloven, alt efter hvorvidt sikkerheden af personlige data er brudt. Dette betyder ikke blot, at samme hændelse skal indberettes til forskellige myndigheder, men disse myndigheder kan endda være i forskellige medlemsstater alt efter den gældende jurisdiktion for UDT'en ifølge de to love. Vi anbefaler, at medlemsstaterne anerkender behovet for og stræber efter at tilvejebringe en enkelt hændelsesunderretning, og at de søger at oprette kommunikationskanaler for at dele relevant information imellem sig, uden at den forretningsmæssige fortrolighed overtrædes.

- De kompetente myndigheder bør tage højde for de omdømmemæssige og kommercielle følger for UDT'en, inden de deler information om hændelser med offentligheden. Endnu mere vigtigt er, at en offentliggørelse af hændelsen muligvis kan forøge sikkerhedsrisikoen. Det er derfor vigtigt at koordinere med de involverede aktører inden en eventuel offentliggørelse.

- I direktivet fremhæves det, at information, der betragtes som fortrolig, skal behandles som sådan (Betragtning 41 og 59, Artikel 1.5).

- I artikel 16.3 understreges det, at underretningen om sikkerhedshændelser ikke må udsætte den underrettende part for øget risiko.

2. Væsentlige operatører

a) Videreudbredelse af sikkerhedsforanstaltninger

- UDT'er, der har OVT'er som kunder, vil blive underlagt de gældende sikkerhedsforanstaltninger, der følger af de væsentlige operatørers lovfastsatte forpligtelser (Artikel 14.1) i forbindelse med forhandlinger af kontrakter. De kan således indirekte blive underlagt deres kunders nationale lovgivning, uanset hvilken lov der gælder i det land, hvor de har deres europæiske hovedsæde.

- Som følge heraf vil alle bestræbelser på at harmonisere sikkerhedsforanstaltningerne for væsentlige operatører være velsete. Selvom medlemsstaterne er berettigede til at pålægge de væsentlige operatører strengere forpligtelser end de, der er anført i direktivet (Artikel 3), anbefaler vi, at der udvises mådehold hermed, og vi tilskynder medlemsstaterne til at arbejde hen imod en harmoniseret tilgang. Dette kan opnås ved at undgå at indføre yderligere foranstaltninger i de nationale gennemførelser og ved at søge at fastlægge passende sikkerhedsforanstaltninger i samarbejdsgruppen i stedet for at fokusere på den nationale proces.

- Sikkerhedskravene skal så vidt muligt baseres på internationale standarder (såsom ISO 27x-serien) og anerkendte bedste sikkerhedspraksis.

- De sikkerhedsforanstaltninger, der pålægges OVT'erne, må under alle omstændigheder ikke kræve, at særlige IKT-produkter designes, udvikles eller fremstilles på en bestemt måde (Betragtning 51).

b) Videreudbredelse af underretning om sikkerhedshændelser

- Operatørerne af væsentlige tjenester er forpligtede til at underrette om sikkerhedshændelser hos de UDT'er, de har kontrakt med, når disse påvirker kontinuiteten af deres væsentlige tjenester (Artikel 16.5). UDT'erne skal derfor være kontraktligt forpligtede til at underrette de betragtede væsentlige operatører om sikkerhedshændelser, der måtte påvirke dem.

- Vi sætter pris på den fleksibilitet mht. tidsplanen for OVT'ernes underretning, der er ligger i udtrykket "hurtigst muligt" (Artikel 14.3). De nationale gennemførelser bør ikke indføre særlige tidsfrister, og hvis OVT'erne bliver bedt om at begrunde den tid, underretningen tager, skal den periode, i forhold til hvilken de bedømmes, i alle tilfælde starte fra det tidspunkt, hvor OVT'en blev gjort opmærksom på hændelsen, ikke hvor UDT'en blev opmærksom på den.

- I artikel 14.7 forudses det, at samarbejdsgruppen udarbejder retningslinjer om omstændighederne for underretningen i modsætning til Kommissionens harmoniserende rolle for UDT'ernes underretninger. I betragtning af UDT'ernes dobbelte anmeldelsespligt er det vigtigt, at de respektive underretningskrav ikke er modstridende, og at de stemmer så godt overens som muligt. Denne proces skal således bedømmes i forhold til dette mål. UDT'ernes underretningskrav skal desuden overholde deres fortrolighedspligt over for deres OVT-kunder og må ikke forlange, at de deler fortrolige forretningsoplysninger.

OM DIGITALEUROPE

DIGITALEUROPE repræsenterer den digitalteknologiske industri i Europa. Vores medlemmer omfatter nogle af verdens største IT-, telekommunikations- og forbrugerelektronikfirmaer samt nationale foreninger fra alle dele af Europa. DIGITALEUROPE ønsker, at Europas selskaber og borgere får maksimalt udbytte af de digitale teknologier, og at Europa opfostrer, tiltrækker og opretholder verdens bedste selskaber inden for digital teknologi.

DIGITALEUROPE sikrer industriens deltagelse i udviklingen og gennemførelsen af EU's politik. DIGITALEUROPE's medlemmer omfatter 62 firmaer og 37 nationale brancheforeninger fra hele Europa. Vores websted giver yderligere oplysninger om vores seneste nyheder og aktiviteter: http://www.digitaleurope.org

MEDLEMSSKAB AF DIGITALEUROPE

Firmamedlemmer

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

Nationale brancheforeninger

Belgien: AGORIA
Bulgarien: BAIT
Cypern: CITEA
Danmark: DI Digital, IT-BRANCHEN
Estland: ITL
Finland: FFTI
Frankrig: AFNUM, Force Numérique, Tech in France
Grækenland: SEPE
Hviderusland: INFOPARK
Irland: ICT IRELAND
Italien: ANITEC
Litauen: INFOBALT
Nederlandene: Nederland ICT, FIAR
Polen: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Rumænien: ANIS, APDETIC
Schweiz: SWICO
Slovakiet: ITAS
Slovenien: GZS
Spanien: AMETIC
Storbritannien: techUK
Sverige: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Tyrkiet: Digital Turkey Platform, ECID
Tyskland: BITKOM, ZVEI
Ukraine: IT UKRAINE
Ungarn: IVSZ
Østrig: IOÖ

DIGITALEUROPE
Rue de la Science, 14 - 1040 Bruxelles [Belgien]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Medlem af Kommissionens åbenhedsregister: 64270747023-20